Rechts- und ethikkonforme Identifikation von unternehmensschädlichen Handlungen durch semiautomatisierte Prozesse

Benedikt Lebek
Stefan Hoyer
Halyna Zakhariya
Michael H. Breitner

Veröffentlicht in:
Multikonferenz Wirtschaftsinformatik 2012
Tagungsband der MKWI 2012
Hrsg.: Dirk Christian Mattfeld; Susanne Robra-Bissantz

Braunschweig: Institut für Wirtschaftsinformatik, 2012

Rechts- und ethikkonforme Identifikation von unternehmensschädlichen Handlungen durch semiautomatisierte Prozesse

Benedikt Lebek

Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, 30167 Hannover,
E-Mail: lebek@iwi.uni-hannover.de

Stefan Hoyer

Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, 30167 Hannover,
E-Mail: hoyer@iwi.uni-hannover.de

Halyna Zakhariya

Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, 30167 Hannover,
E-Mail: zakhariya@iwi.uni-hannover.de

Michael H. Breitner

Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, 30167 Hannover,
E-Mail: breitner@iwi.uni-hannover.de

Abstract

Heutzutage werden in einem Unternehmen eine Vielzahl sensibler Informationen und Daten verarbeitet, die auch vor Attacken aus dem Inneren des Unternehmens geschützt werden müssen. Ein Umdenken im (IT-) Risikomanagement hin zu einer präventiven Identifikation von potenziell unternehmensschädlichen Handlungen wird bereits in der Literatur diskutiert und setzt u. a. starke Mitarbeiterüberwachungen voraus. Dies stößt auf datenschutzrechtliche Grenzen und wirft ethische sowie moralische Bedenken auf. Mit Fokus auf Compliance des (IT-) Risikomanagement wird in diesem Aufsatz gezeigt, wie ein Modell zur automatisierten Identifikation und Prävention unternehmensschädlicher Handlungen aussehen kann, insbesondere wenn deutsches Datenschutzrecht und Mitbestimmungsrechte der Arbeitnehmer beachtet sowie ethische und moralische Bedenken berücksichtigt werden.

1 Einleitung

In der modernen, global vernetzten Wirtschaftswelt werden nahezu alle Geschäftsprozesse auf elektronischem Weg vollzogen. Dabei entstehen eine Vielzahl sensibler Informationen und Daten, die von hohem Wert für das jeweilige Unternehmen sind [13]. Daher ist der

Schutz dieser Daten und Informationen gegen Diebstahl, Verlust, Manipulation oder andere Angriffe notwendig. In diesem Zusammenhang rückt die Betrachtung von Angriffen durch Insider stärker in den Fokus. So sehen Unternehmen Angriffe durch Mitarbeiter (Insider) als zweitgrößte Bedrohung nach Hackerangriffen [10]. Eine notwendige Folge ist die Einrichtung von Überwachungsmaßnahmen innerhalb der Unternehmen [8]. In der Praxis steht derzeit noch die Identifizierung von Insidern nach Durchführung einer unternehmensschädlichen Handlung im Vordergrund („Insider Threat Detection“) [7]. Jedoch liefern diese Methoden oftmals erst ein Ergebnis, wenn bereits ein irreparabler, manchmal existenzgefährdender Schaden für das Unternehmen entstanden ist. In einer schnelllebigen Geschäftswelt, in der u. a. Echtzeit-Informations- und -buchungssysteme eingesetzt werden, wird nach einer zeitnahen Identifikation von unternehmensschädlichen Handlungen verlangt [11]. Ein Umdenken im (IT-) Risikomanagement hin zu einer präventiven Identifikation von potenziellen unternehmensschädlichen Handlungen („Insider Threat Prediction“) wird bereits in der Literatur diskutiert. Zu diesem Zweck werden in automatisierten Prozessen Kennzahlen und Risikomaße für die Bedrohung berechnet, die von einzelnen Insidern ausgeht. Die Berechnung basiert auf der statistischen Analyse vorher festgelegter Szenarien und setzt Verhaltensanalysen und Mitarbeiterüberwachungen voraus. Bei der Überwachung wird auf teils sensible Informations- und Datenquellen, wie beispielsweise E-Mail-Inhalte, zurückgegriffen. Eine derart intensive Mitarbeiterüberwachung stößt auf datenschutzrechtliche Grenzen und wirft ethische sowie moralische Bedenken auf. Es entsteht ein Spannungsfeld zwischen dem Unternehmensinteresse unternehmensschädliche Handlungen abzuwehren und dem Recht des einzelnen Mitarbeiters auf Schutz seiner Privatsphäre. Die Brisanz des Themas belegen die Fälle bei der Deutschen Telekom und der Deutschen Bahn im Jahr 2009. Dort haben die Verletzungen des Datenschutzrechtes für Schlagzeilen gesorgt, als u. a. Kontodaten von Mitarbeitern mit denen von Zulieferern verglichen worden sind [2].

Vor dem Hintergrund der konkurrierenden Interessen von Arbeitgebern und Arbeitnehmern bekommt das Thema der Compliance im (IT-) Risikomanagement eine immer höhere Bedeutung. Fraglich ist die Möglichkeit des Aufbaus eines automatisierten „Insider Threat Prediction and Detection“-Systems, welches das Mitarbeiterverhalten überwacht und dabei sowohl rechtliche als auch moralische Anforderungen erfüllt. Ziel dieses Aufsatzes ist die Erweiterung des Modells von Greitzer et al. [7] durch Elemente anderer in der Literatur verbreiteter Modelle und selbst konzipierte Komponenten. Der hier vorgestellte Lösungsansatz berücksichtigt dabei speziell die in Deutschland geltenden rechtlichen Rahmenbedingungen.

2 Literaturanalyse und Status quo

In der Literatur gibt es eine Reihe von Autoren, die sich mit dem Thema „Insider Threat Prediction and Detection“ beschäftigen. Die in den letzten Jahren veröffentlichten Modelle zeigen unterschiedliche Herangehensweisen an die automatisierte Identifikation und Prävention unternehmensschädlicher Handlungen und beleuchten meist nur bestimmte Teilaspekte. Auch die Problematik der rechtlichen Grenzen und ethischen sowie moralischen Bedenken wird unterschiedlich berücksichtigt.

So fokussieren Magklaras/Furnell [12] ihre Arbeit auf der Vorhersage unternehmensschädlicher Handlungen. Insbesondere konzentrieren sie sich darauf, die Anzeichen einer möglichen Bedrohung zu erkennen, zu analysieren und zu interpretieren. Zu diesem Zweck werden u.a.

persönliche Daten und Informationen herangezogen, wie beispielsweise besondere Fähigkeiten eines Mitarbeiters. Das Modell nennt mögliche Quellen zur Erhebung der Daten und Informationen und liefert ein Vorgehen zu deren Interpretation. Ethische, moralische und rechtliche Grenzen der Mitarbeiterüberwachung bleiben trotz Verwendung persönlicher Daten und Informationen unberücksichtigt.

Althebyan und Panda [14] präsentieren ebenso ein Modell zur Vorhersage unternehmensschädlicher Handlungen. Als Grundlage dienen Daten des IT-Monitorings, insbesondere die Auswertung von Dokumentzugriffsprotokollen. Hierbei erfolgt ein Abgleich der getätigten Zugriffe mit den je nach Zugehörigkeit zur Organisationsstruktur vergebenen Berechtigungen. Da lediglich die Zugriffe von Mitarbeitern auf Dokumente überwacht werden und andere Faktoren unberücksichtigt bleiben, wird das Thema der rechtlichen Grenzen und ethischen sowie moralischen Bedenken in diesem Modell weitgehend vernachlässigt.

Die Verknüpfung der Daten des IT-Monitorings auf der einen Seite mit den psychologischen Mitarbeiterprofilen auf der anderen Seite liefert das von Kandias et al. (2010) [9] beschriebene Prognosemodell. Mit Hilfe eines Entscheidungsalgorithmus werden Hinweise darauf gewonnen, ob sich ein Mitarbeiter verdächtig verhält und intensiver beobachtet werden sollte. Auf die Frage nach dem Datenschutz und der Wahrung der Privatsphäre der Angestellten sowie mögliche Quellen für psychologische Mitarbeiterinformationen gehen die Autoren nicht näher ein.

Das Modell von Islam et al. [8] ermöglicht die Aufdeckung von unternehmensschädlichen Handlungen in ERP-Systemen. Dabei werden Daten und Informationen aus ERP-Logfiles mit vorher definierten Betrugsszenarien verglichen. Aufgrund der reinen Untersuchung von Logfiles, stellt das Modell datenschutzrechtlich ein geringeres Problem dar, als Modelle, die auch andere persönliche Daten und Informationen von Mitarbeitern einbeziehen. Eine Schwachstelle des Modells können die vordefinierten Betrugsszenarien sein. Da neuartige Betrugsformen nach einem noch unbekannten Muster erfolgen können, werden diese möglicherweise nicht durch die definierten Szenarien erkannt.

Flegel [6] schlägt in seinem Modell die Pseudonymisierung von Auditdaten vor, um eine datenschutzrechtlich unbedenkliche Überwachung sämtlicher Daten und Informationen zu ermöglichen. Das Modell stellt somit keine Vorgehensweise zur Aufdeckung von unternehmensschädlichen Handlungen im eigentlichen Sinne dar, sondern beschäftigt sich ausschließlich mit dem organisatorischen Ablauf des Pseudonymisierungsprozesses.

Greitzer et al. [7] entwickeln ein Konzept zur Erstellung von Insider-Profilen anhand der Kombination von Daten des IT-Monitorings mit psychosozialen Mitarbeiterinformationen. Um rechtliche und ethische Barrieren der Einbindung von psychosozialen Informationen zu überwinden, schließen die Autoren von vornherein einige Quellen für psychosoziale Daten und Informationen aus. Hierzu zählen u. a. Vorstrafenregister oder Krankenakten. Jedoch können auch die explizit vorgeschlagenen Quellen nicht ohne Weiteres als rechtlich zulässig und ethisch vertretbar angesehen werden.

Tabelle 1 gibt ein Überblick über die beschriebenen Modelle anhand ausgewählter Vergleichskriterien. Dabei wird unterschieden, ob das jeweilige Modell unternehmensschädliche Handlungen vorhersagt („Prediction“) oder nachträglich aufdeckt („Detection“). Weiterhin werden die Modelle hinsichtlich der Art der eingesetzten Datenquellen (IT-Monitoring-, persönliche- oder psychosoziale Daten) klassifiziert. Die Ausrichtung der jeweiligen Modelle

auf die Erkennung von absichtlichen („Intentional“) oder unabsichtlichen („Accidential“) unternehmensschädlichen Handlungen stellen weitere Vergleichsmöglichkeiten dar. Anhand der Modellgegenüberstellung ist beispielsweise deutlich zu sehen, dass Ethik und Recht nur wenig Berücksichtigung finden. Diese beiden Kriterien sind gerade für die Vorhersage von Bedeutung. Da hierbei bereits vor Umsetzung einer unternehmensschädlichen Handlung Analysen durchgeführt werden, können zunächst auch unschuldige Personen in Verdacht geraten. Daraus folgt die Frage, ob trotzdem einzelne Komponenten der hier aufgeführten Modelle in ein „Insider Threat Prediction and Detection“-Modell übernommen werden können, das insbesondere deutsche Datenschutzbestimmungen erfüllt und ethische sowie moralische Bedenken berücksichtigt. Eine mögliche Lösung wird anhand einer Erweiterung des Modells von Greitzer et al. [7] im folgenden Kapitel präsentiert.

Autor(en) / Kriterium	Magklaras/ Furnell [12]	Althebyan/ Panda [1]	Kandias et al. [9]	Islam et al. [8]	Flegel [6]	Greitzer et al. [7]
Prediction	x	x	x			x
Detection		x		x	o	x
Daten des IT-Monitorings	x	x	x	x	x	x
Persönliche Informationen	x		x			x
Psychologische Informationen			x			x
Intentional	x	x	x	x	x	x
Accidential	x	x		x	x	x
Ethik						o
Recht			x		x	o

Legende: x = Kriterium erfüllt; o = Kriterium teilweise erfüllt

Tabelle 1: Modellvergleich (eigene Darstellung)

3 Modellerweiterung

Um die Anforderungen insbesondere des deutschen Rechts sowie der Ethik und Moral zu erfüllen, wird das von Greitzer et al. [7] erstellte Modell erweitert. Dieses Modell ist aufgrund seines ausreichend hohen Abstraktionsniveaus für eine allgemeingültige Betrachtung und Erörterung der problematischen Elemente der „Insider Threat Prediction and Detection“ geeignet. Auf diese Weise wird eine Diskussion von rechtlichen Grenzen bzw. ethisch und moralischen Bedenken vermieden, die sich zu spezifisch auf ein bestimmtes Modell bezieht und von daher nicht auf ein breites Interesse stößt. Des Weiteren werden bei Greitzer et al. Daten des IT-Monitorings mit psychosozialen Informationen kombiniert.

Die Berücksichtigung von psychologischen und persönlichen Daten und Informationen stellt den wohl strittigsten Punkt bei der „Insider Threat Prediction and Detection“ dar. Da nach deutschem Datenschutzrecht eine vollständig automatisierte Entscheidungsfindung nicht gestattet ist, wird im Weiteren eine manuelle Komponente in das „Insider Threat Prediction

and Detection“-System eingeführt. Durch die Abkehr von einem ausschließlich automatisierten Prozess, wird ein „Semiautomatic Insider Threat Prediction and Detection System“ (SITPDS) geschaffen. Bild 1 stellt das im Folgenden beschriebene Modell inklusive der Erweiterungen dar.

3.1 Insider Threat Prediction and Detection Management (ITPDM)

Den Hauptbestandteil der manuellen Komponente des SITPDS bildet das „Insider Threat Prediction and Detection Management“ (ITPDM). Das ITPDM stellt eine organisatorische Einheit dar, die sich an dem von Kandias et al. [9] vorgestellten „Management Team“ orientiert. Somit bildet das ITPDM eine Stelle bzw. Abteilung im Unternehmen, deren Aufgabe primär in der Koordination und Durchführung der Identifikation von unternehmensschädlichen Handlungen durch Mitarbeiter besteht. Aufgabe des ITPDM ist die Sicherstellung der Einhaltung von Anforderungen, die der Gesetzgeber an die inhaltliche Prüfung von automatisierten Entscheidungen stellt. Zur Wahrung der Unabhängigkeit ist diese Abteilung direkt der Unternehmensführung unterstellt.

Bevor geeignete Maßnahmen als Reaktion auf automatisierte Entscheidungen ergriffen werden können, muss zunächst das gemäß § 6 a Abs. 2 des Bundesdatenschutzgesetzes (BDSG) geforderte dreistufige Verfahren angewendet werden. Bei diesem Verfahren muss der Betroffene über das Vorliegen einer Entscheidung, die Begründung für diese Entscheidung und die Möglichkeiten der Anfechtung informiert werden [2]. Zur Erfüllung dieser Aufgabe wird innerhalb des ITPDM eine Anlaufstelle eingerichtet. Darüber hinaus kommen dem ITPDM weitere Aufgaben im Bereich der Prozessanpassung und -verbesserung zu. Das ITPDM hat beispielsweise dafür Sorge zu tragen, dass der „Insider Threat Prediction“-Prozess stets den technischen und rechtlichen Rahmenbedingungen angepasst wird. Eine weitere wichtige Aufgabe des ITPDM ist die Etablierung und Förderung des Sicherheitsbewusstseins in der Belegschaft durch geeignete Maßnahmen. Dies ist notwendig, da es neben absichtlichen unternehmensschädlichen Handlungen auch solche gibt, die aus Versehen, Unwissenheit oder Ignoranz [13] geschehen.

3.2 Daten- und Informationsquellen

Neben der Forderung nach einer möglichst hohen Effizienz der „Insider Threat Prediction and Detection“, steigern auch die rechtlichen und ethischen sowie moralischen Rahmenbedingungen die Bedeutung der Quellenauswahl. Nicht jede technisch mögliche Daten- und Informationsquelle ist von vornherein auch aus rechtlicher, ethischer oder moralischer Sicht akzeptabel. Daten- und Informationsquellen können grundsätzlich in drei Kategorien unterteilt werden.

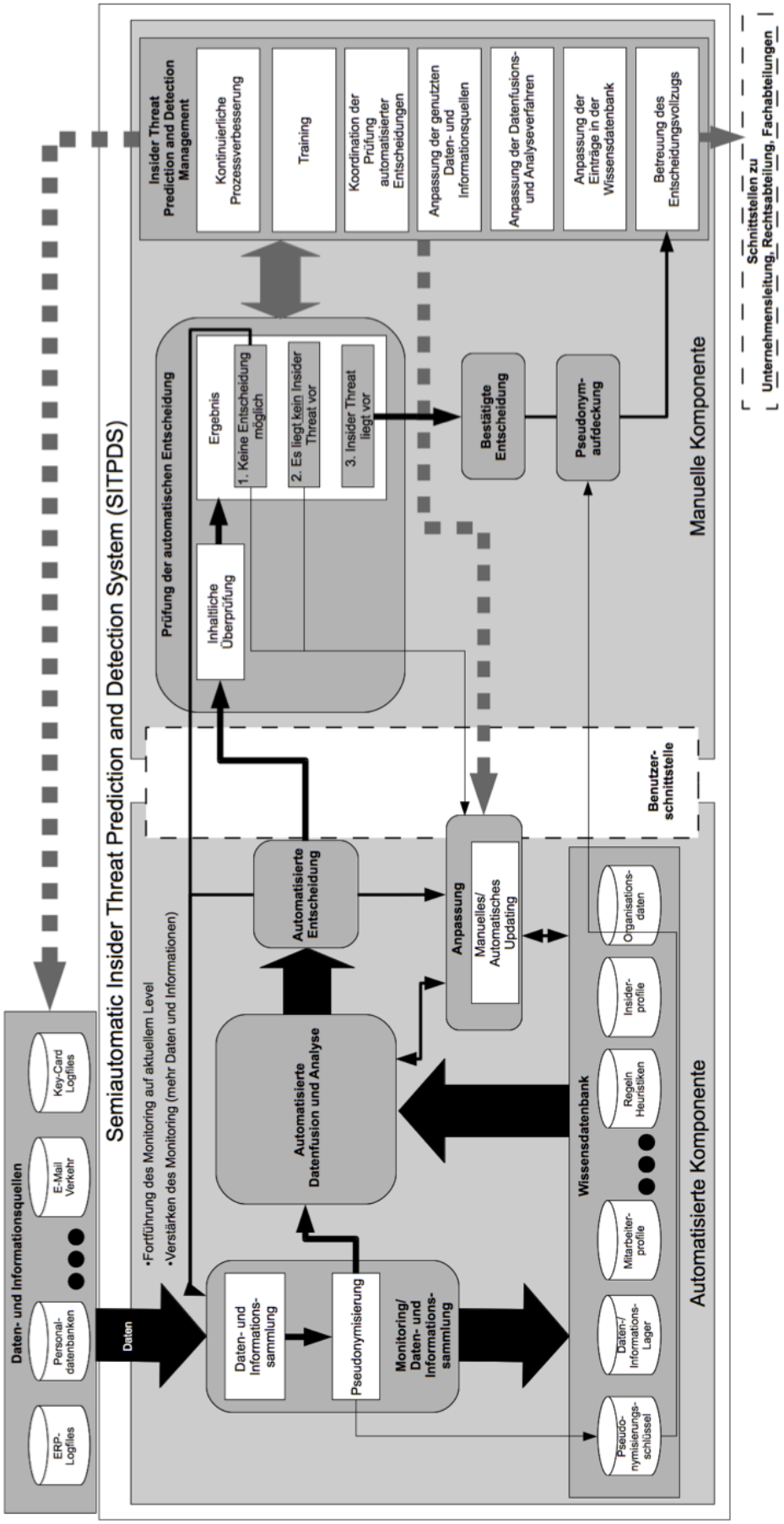

Bild 1: SITPDS Modell (eigene Darstellung in Anlehnung an [7])

Zum einen gibt es Quellen, welche die rechtlichen und ethischen Rahmenbedingungen nicht verletzen und daher uneingeschränkt zur „Insider Threat Prediction and Detection“ genutzt werden können. Darunter fallen Quellen, die einen eher technischen Hintergrund besitzen, wie beispielsweise die Auswertung von Zeiterfassungskarten oder die Protokollierung über Gebäudezutritte und Quellen, die einen starken Personenbezug haben. In diesem Zusammenhang sind Profile zu sehen, die auf Basis des Feedbacks von Vorgesetzten oder anderen Mitarbeitern erstellt werden sowie die Überwachung von Leistungen, Fähigkeiten und Disziplin oder gar Hintergrundüberprüfungen [3].

Unter die zweite Kategorie fallen Daten- und Informationsquellen, die ausschließlich beim Vorliegen bestimmter Sachverhalte zulässig sind. Eine Totalüberwachung der Mitarbeiter ist grundsätzlich unzulässig. Da die Nutzung einiger Quellen einen so intensiven Eingriff in die Privatsphäre des Arbeitnehmers bedeutet, überwiegt nicht von vornherein das Interesse des Arbeitgebers. Beim Vorliegen bestimmter Bedingungen gewinnt das Arbeitgeberinteresse jedoch an Gewicht. Eine solche Bedingung kann beispielsweise ein konkreter Verdacht hinsichtlich der Durchführung oder Planung einer unternehmensschädlichen Handlung durch einen bestimmten Mitarbeiter sein [4].

Des Weiteren existieren Quellen, die aufgrund der Intensität des Eingriffs in die Privatsphäre des Mitarbeiters generell ausgeschlossen werden müssen. Hierzu zählen beispielsweise ärztliche oder psychologische Gutachten sowie Informationen aus Führungszeugnissen [3]. Für die Nutzung dieser Quellen muss ein direkter Bezug der begangenen Straftat mit der ausgeübten Tätigkeit bestehen [5]. Zur Vermeidung von rechtlichen Schwierigkeiten ist die frühzeitige Festlegung der für das SITPDS zu nutzenden Daten- und Informationsquellen notwendig.

3.3 Sammlung und Pseudonymisierung von Daten und Informationen

Auch wenn schon vor Beginn der Daten- und Informationssammlung festgelegte Quellen als rechtlich und moralisch unbedenklich gelten, ist weiterhin zu beachten, dass die Vollkontrolle eines Mitarbeiters ohne konkreten Verdacht auf eine unternehmensschädliche Handlung nicht zulässig ist. Obgleich die Daten- und Informationenquellen im SITPDS generell als zulässig eingestuft werden, ist eine Pseudonymisierung in Anlehnung an das von Flegel [6] vorgestellte Verfahren empfehlenswert. Die Umkehrung der Pseudonymisierung darf solange niemandem möglich sein, bis eine Reidentifizierung aufgrund der Ergebnisse des Entscheidungsprozesses ausdrücklich erlaubt ist. Zur Reidentifizierung berechtigte Ergebnisse des Entscheidungsprozesses, sind vorab genau festzulegen. Des Weiteren muss trotz der Pseudonymisierung gewährleistet sein, dass im Analyseprozess unternehmensschädliche Handlungen mit der gleichen Präzision entdeckt werden können, wie es mit den Originaldaten und -informationen möglich ist.

3.4 Entscheidungsprozess

Das SITPDS beinhaltet einen automatisierten und einen manuellen Entscheidungsprozess. Den Kern des automatisierten Entscheidungsprozesses (siehe Bild 2) bildet die Daten- und Informationsanalyse. Hier wird an dem von Greitzer et al. [7] entwickelten Vorgehen festgehalten, indem aus der Beobachtung von Daten und Informationen Indikatoren abgeleitet werden. Daraus können Rückschlüsse auf ein bestimmtes Mitarbeiterverhalten gezogen werden. Dabei werden Daten und Informationen aus dem psychologischen Profiling und

IT-Nutzer-Profiling verwendet, wie beispielsweise von Kandias et al. [12] beschrieben. Daten und Informationen des IT-Monitorings können u. a. die Zugriffe eines Mitarbeiters auf bestimmte zugriffsbeschränkte Dateien sein. Anschließend können mit der Methode von Althebyan/Panda [14] mögliche Bedrohungen vorhergesagt werden. Auch ein Abgleich des aufgezeichneten realen Verhaltens von Mitarbeitern mit zuvor festgelegten Insider-Profilen ist an dieser Stelle denkbar. Ergebnis des automatisierten Analyseprozesses ist eine Entscheidung, ob eine unternehmensschädliche Handlung vorliegt, weitere Daten und Informationen benötigt werden oder keine Bedrohung zu erkennen ist. Diese Entscheidung ist mit Risiko-Scorewerten bzw. Risikomaßen begründet, die nach Verfahren berechnet werden, wie beispielsweise von Magklaras/Furnell [12] oder Kandias et al. [9] vorgestellt.

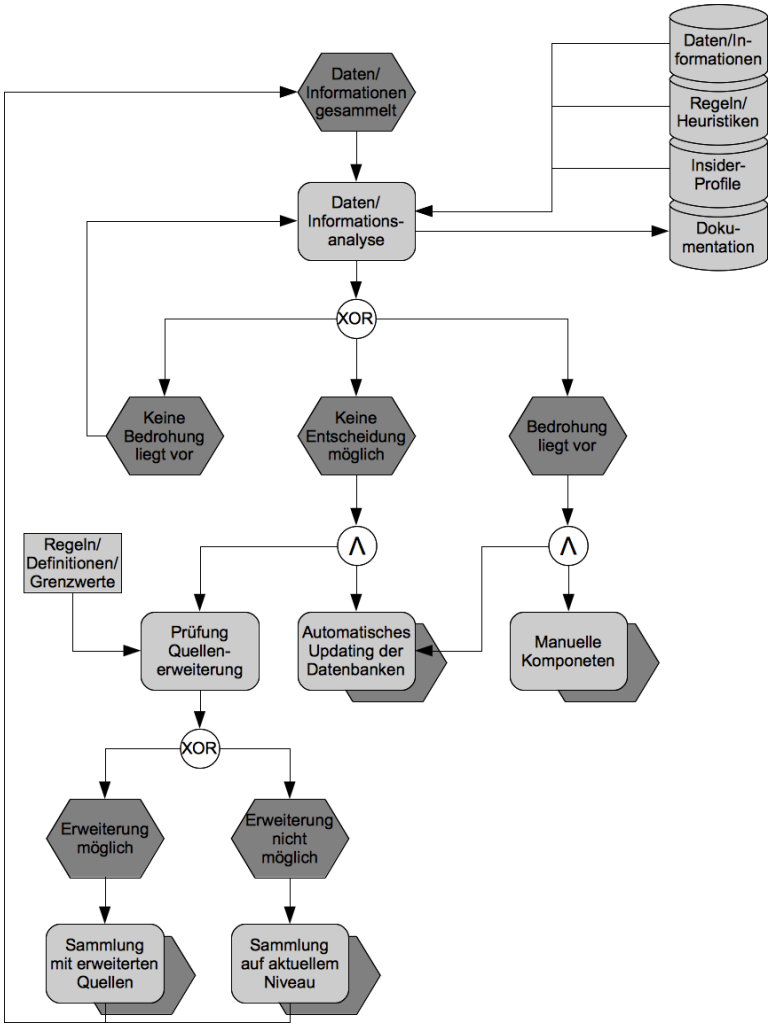

Bild 2: EPK-Diagramm des automatisierten Entscheidungsprozess (eigene Darstellung)

Während der Daten- und Informationsanalyse ist eine ausführliche Dokumentation der verwendeten Daten und Informationen, der Analysemethoden und des Ablaufs der Analyse wichtig. Dies ist notwendig für die anschließende inhaltliche Kontrolle der automatisierten Entscheidung durch eine natürliche Person. Eine manuelle, inhaltliche Kontrolle erfolgt, wenn die automatisierte Analyse zu dem Ergebnis gekommen ist, dass eine unternehmensschädliche Handlung vorliegt. In einem solchen Fall wird auch die Wissensdatenbank automatisch aktualisiert, indem neue Erkenntnisse zu vordefinierten Insider-Profilen gespeichert werden.

Wenn keine Entscheidung durch die automatisierte Analyse gefällt werden kann, findet sowohl ein Update der Wissensdatenbank statt als auch die Prüfung, ob weitere Quellen zur Daten- und Informationsbeschaffung herangezogen werden können. Dies ist denkbar, wenn beispielsweise eine bestimmte Wahrscheinlichkeit für das Vorliegen einer unternehmensschädlichen Handlung berechnet worden ist, welche aber noch nicht zur endgültigen Bestätigung einer Bedrohung ausreicht. Ist eine Quellenerweiterung möglich, wird der Analyseprozess mit den zusätzlichen Daten und Informationen aus den hinzugezogenen Quellen erneut durchlaufen. Reichen die Bedingungen nicht für eine Erweiterung der Quellen aus oder liegen keine Anzeichen für eine unternehmensschädliche Handlung vor, wird das Analyseverfahren mit den bisherigen Quellen weiter durchlaufen.

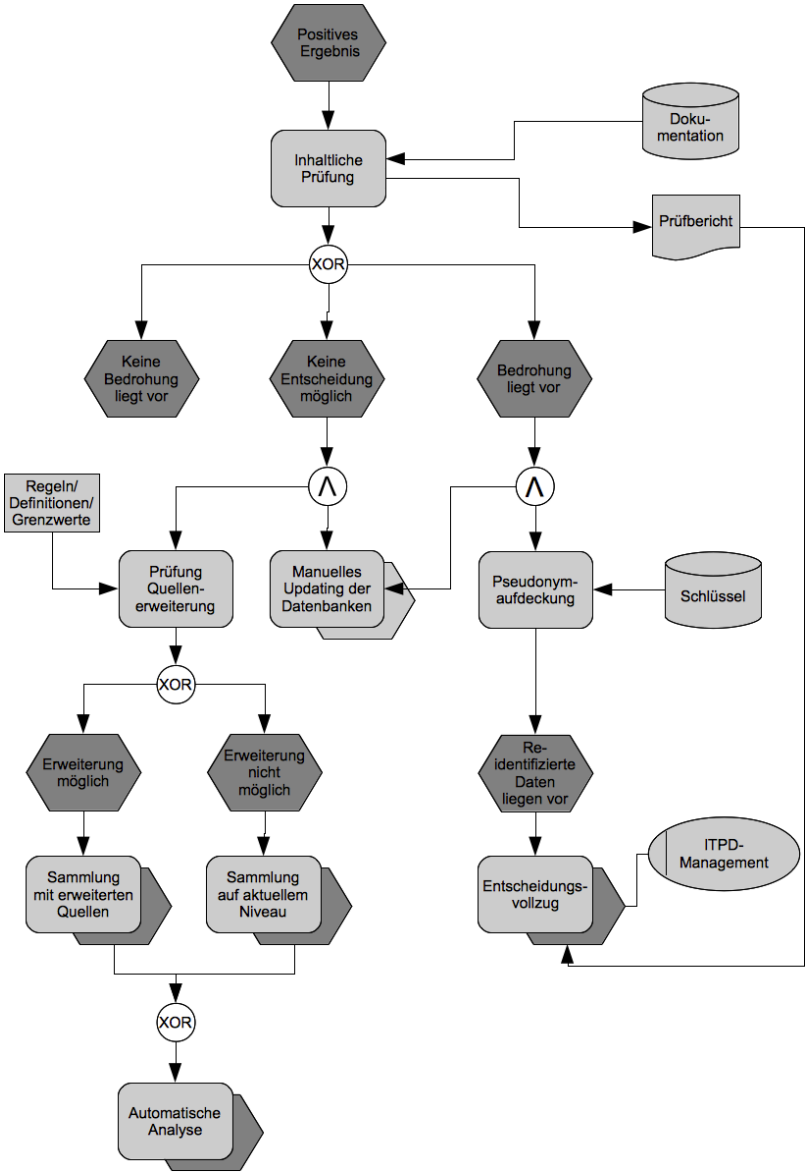

Bild 3: EPK-Diagramm des manuellen Prüfungsprozesses (eigene Darstellung)

Der manuelle Entscheidungsprozess ist dem automatisierten Entscheidungsprozess direkt nachgelagert. Er ist notwendig, da eine vollständig automatisierte Entscheidungsfindung durch § 6 a BDSG verboten ist [2]. Der manuelle Prozess beginnt, sobald eine positive automatisierte Entscheidung vorliegt (siehe Bild 3). Positiv in diesem Zusammenhang bedeutet,

dass laut dem Ergebnis der automatisierten Daten- und Informationsanalyse konkrete Hinweise auf eine unternehmensschädliche Handlung vorliegen. Den Kern des manuellen Entscheidungsprozesses stellt die inhaltliche Prüfung der automatisierten Entscheidung dar. Dabei muss durch eine natürliche Person überprüft werden, ob das positive Ergebnis der automatisierten Daten- und Informationsanalyse gerechtfertigt ist. Hierzu muss die prüfende Person eine entsprechende Befugnis besitzen und Zugriff auf die notwendigen Daten und Informationen zum Nachvollzug der automatisierten Entscheidung haben [16]. Aus diesem Grund werden die verwendeten Daten und Informationen, die Analysemethoden und der Ablauf der Analyse während der automatisierten Prüfung dokumentiert.

Während der manuellen inhaltlichen Prüfung wird ein Bericht erstellt, der für die spätere Begründung der Entscheidung von Bedeutung ist. Die möglichen Ergebnisse der inhaltlichen Prüfung der Entscheidung können denen der automatisierten Analyse entsprechen. Liegt entgegen der automatisierten Entscheidung keine Bedrohung vor, endet der Prozess.

Kann der Prüfer anhand der vorliegenden Daten und Informationen keine Entscheidung treffen, ist das Hinzuziehen weiterer Quellen zu eruieren. Das Vorgehen entspricht dem des automatisierten Entscheidungsprozesses. Zur Verbesserung der Qualität zukünftiger automatisierter Entscheidungen, wird im Gegensatz zum vollständig automatisierten Entscheidungsprozess bei jeder manuellen inhaltlichen Prüfung die Wissensdatenbank aktualisiert. Bestätigt die manuelle, inhaltliche Prüfung die automatisierte Entscheidung, werden die pseudonymisierten Daten und Informationen reidentifiziert. Auf dieser Basis kann nun das ITPDM mit der Durchführung geeigneter Maßnahmen beginnen.

4 Diskussion

Das wichtigste Element des SITPDS ist die Einführung einer manuellen Komponente. Durch die Abkehr von einem vollständig automatisierten Prozess zur „Insider Threat Prediction and Detection“ kann ein semiautomatisiertes Modell präsentiert werden, welches die in Deutschland geltenden rechtlichen Grenzen einhält und ethische sowie moralische Bedenken berücksichtigt. Die manuelle Komponente ist für die Konfiguration, kontinuierliche Verbesserung und Anpassung der automatischen Komponente sowie der Daten- und Informationsquellen zuständig. Darüber hinaus ist diese für die Überprüfung und die Durchsetzung der automatisierten Entscheidungen aus rechtlichen Gründen notwendig.

Im Gegensatz zu rechtlichen Grenzen, die auf der Prozessebene Anwendung finden, spielen Ethik und Moral auf einer übergeordneten Ebene eine Rolle. Ethische und moralische Bedenken treten auf, wenn über die Einführung eines „Insider Threat Prediction and Detection“-System entschieden werden soll. Im Vordergrund steht hierbei die Abwägung der Persönlichkeitsrechte von Mitarbeitern und anderen Insidern gegenüber den Rechten von Stakeholdern, wie beispielsweise Eigentümern. Um ein Arbeitsklima des gegenseitigen Vertrauens zu schaffen und eine gute Sicherheitskultur innerhalb des Unternehmens zu entwickeln, ist die aktive Beteiligung von Mitarbeitern am Sicherheitskonzept unabdingbar [14].

Die Fokussierung auf die Anforderungen der deutschen Gesetzgebung stellt eine Schwachstelle des hier präsentierten Modells dar. Für andere Rechtsräume kann eine Anpassung des Modells notwendig sein. Dies ist vor allem für international tätige Unternehmen wichtig, deren Standorte auf mehrere Länder und somit unterschiedliche Rechtsräume verteilt sind.

Damit das diskutierte Modell trotz seines hohen Abstraktionsniveaus in der Praxis Anwendung finden kann, ist ein Herunterbrechen auf die Anwendungsebene und die Entwicklung realisierbarer Tools und Analyseverfahren notwendig. Auch konkrete Organisationsstrukturen und -abläufe müssen noch erarbeitet werden, da aus dem Prozess zur Identifikation unternehmensschädlicher Handlungen ernsthafte Rechtsfolgen für die Betroffenen erwachsen. Ein weiterer wichtiger Punkt für den Praxiseinsatz eines SITPDS ist das Verhältnis zwischen Kosten und Nutzen einhergehender Präventionsmaßnahmen.

5 Fazit

Bei der Betrachtung von verschiedenen Modellen zur „Insider Threat Prediction and Detection“ wird deutlich, dass es derzeit unterschiedliche Herangehensweisen gibt. Jedoch werden die Aspekte von Recht und Moral sowie Ethik nicht ausreichend berücksichtigt. So geht der Großteil der Autoren nicht auf ethische und moralische Bedenken ein. Die rechtlichen Grenzen werden in der Literatur nur im Ansatz behandelt. Dieser Aufsatz zeigt, wie ein System zur „Insider Threat Prediction and Detection“ ausgestaltet werden kann, um den Anforderungen des deutschen Datenschutzrechts und den Mitbestimmungsrechten der Arbeitnehmer sowie den Forderungen von Ethik und Moral gerecht zu werden. Die wichtigste Neuerung dieses Aufsatzes ist die Abkehr von einer vollständig automatisierten „Insider Threat Prediction and Detection“ durch die Einführung eines SITPDS. Zumindest nach deutschem Recht ist die Durchführung eines vollständig automatisierten Prozesses nicht zulässig und die Einführung einer manuellen Komponente notwendig. Dieser Sachverhalt findet bisher in der Literatur wenig Berücksichtigung, was auch darauf zurückzuführen ist, dass sich die Autoren vornehmlich auf den US-amerikanischen Rechtsraum konzentrieren. Zwar ist das Problem der rechtlichen Grenzen und ethischen sowie moralischen Bedenken bekannt, spielt jedoch eine untergeordnete Rolle.

Unternehmensschädliche Handlungen stellen eine starke Bedrohung für Unternehmen dar. Daher kann davon ausgegangen werden, dass die automatisierte Identifikation solcher Bedrohungen in den nächsten Jahren noch weiter an Bedeutung gewinnen wird. Um in der Praxis Anwendung finden zu können, ist die Berücksichtigung von rechtlichen und ethischen sowie moralischen Rahmenbedingungen in den bisher noch sehr theoretischen Modellen notwendig. Das Thema bietet weiteres Forschungspotenzial, u. a. in Bezug auf die Berücksichtigung der berechtigten Interessen aller Beteiligten. Compliance bei „Insider Threat Prediction and Detection“ durch die Berücksichtigung rechtlicher Grenzen und ethischer sowie moralischer Bedenken ist also nicht allein durch technische Maßnahmen zu erreichen, sondern erfordert die Schaffung entsprechender organisatorischer Strukturen und Prozesse.

6 Literatur

[1] Däubler, W (2009): Gläserne Belegschaften? 5. Auflage, Bund-Verlag, Frankfurt am Main.

[2] Gola, P; Schomerus, R (2010): BDSG Kommentar. 10. Auflage, Verlag C. H. Beck, München.

[3] Gola, P; Wronka, G (2010): Handbuch zum Arbeitnehmerdatenschutz. 5. Auflage, Datakontext, Frechen.

[4] Thüsing, G (2010): Arbeitnehmerdatenschutz und Compliance: Verlag C. H. Beck, München.

[5] Wohlgemuth, H (1988): Datenschutz für Arbeitnehmer. 2. Auflage, Luchterhand, Neuwied.

[6] Flegel, U (2010): Privacy Compliant Internal Fraud Screening; In: Pohlmann/Reimer/ Schneider (Hrsg.), *Securing Electronic Business Processes*. Vieweg, Wiesbaden.

[7] Greitzer, FL et al. (2010): Combining Traditional Cyber Security Audit Data with Psychological Data: Towards Predictive Modeling for Insider Threat Mitigiation; In: Probst/Hunker/Gollmann (Hrsg.), *Insider Threats in Cyber Security*. 1. Edition; Springer, Heidelberg.

[8] Islam, A et al. (2010): Fraud Detection in ERP Sytems Using Scenario Matching; In: Rannenberg/Vradharajan/Weber (Hrsg.), *Security and Privacy: Silver Linings in the Cloud: Proceedings of International Information Security Conference (SEC 2010)*. 1. Auflage, Springer, Heidelberg.

[9] Kandias, M et al. (2010): An Insider Threat Prediction Modell; In: Katsikas/Lopez/Soriano (Hrsg.), *Trust, Privacy and Security in Digital Business*; Springer.

[10] CSO Magazine (2008): 2007 E-Crime Watch Survey.

[11] Flowerday, S et al. (2006): Continuous auditing technologies and models: A discussion; Computers & Security Band 25, Juli 2006.

[12] Magklaras, GB; Furnell, SM (2004): A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers & Security Band 24, 2005.

[13] Sarkar, KR (2010): Assessing insider threats to Information security using technical, behavioural and organisational measures. Information Security Technical Report Band 15, August 2010.

[14] Wiele, J (2011): Vertrauensfragen – Unternehmenssicherheit und Führungspraxis. DuD – Datenschutz und Datensicherheit 7/2011.

[15] Althebyan, Q; Panda, B (2007): A Knowledge-Base Model for Insider Threat Prediction. In: United States Military Academy, *Proceedings of the 2007 IEEE Workshop on Information Assurance*. West Point, NY 20-22 June 2007.

[16] Deutscher Bundestag (2008); Drucksache 16/10529, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes.